REMARKS

The Office Action dated May 23, 2005, has been received and carefully noted. The following remarks are submitted as a full and complete response thereto.

Claims 1-21 are pending in the present application and respectfully are submitted for consideration. The Office Action, in paragraph 1, states that claims 14-21 were added by the Response filed February 3, 2005. Applicant notes that claims 14-21 were added in the Response filed June 4, 2004. Further, the Office Action appears to have a typographical error in stating claims 1-22 are pending. Applicant requests that the Examiner confirm claims 1-21 are pending the application.

Claims 1-21 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 6,219,793 (Li et al.) in view of U.S. Patent No. 5,311,596 (Scott et al.). The Office Action took the position that Li taught all the features of the claims except "generating a set of subscriber specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in [] a known mobile communication system." The Office Action then alleged that Scott taught those features missing from Li. Applicant respectfully traverses the obviousness rejection and submits that Li and Scott, either alone or in combination, do not disclose or suggest all the features of any of the presently pending claims.

Claim 1, upon which claims 2-9 are dependent, recites an authentication method for a telecommunications network. The method includes generating a set of subscriber-

specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communications system. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to the terminal. The method also includes choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communications system. The method also includes determining an authenticator with an aid of the chosen key in the terminal. The method also includes transmitting, from the terminal to the network, the authenticator in a data unit. The data unit contains information relating to the manner in which the authentication is formed and notifying the network of which key corresponding to which challenge was chosen. The method also includes determining a check value with the aid of the chosen key in the network. The method also includes comparing the check value with the authenticator.

Claim 10, upon which claims 11-13 are dependent, recites an authentication system for a telecommunications network. The authentication system includes a terminal of the network and first message transmission means for transmitting an authenticator and a data unit to the network. The data unit includes information relating to the manner in which the authenticator is formed. The authentication system also includes checking means for determining a check value with aid of the data unit. The terminal of the

network includes such an identification unit, which receives as input a challenge from which a response and a key are defined essentially in the same manner as in a subscriber identity module of a main mobile communications system. The system also includes generating means for generating authentication data blocks in the same manner as in the mobile communications systems. The authentication data blocks include a challenge, a response and a key. The system also includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal. The terminal includes selection means for selecting one challenge per use. The first message transmission means inserts such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal. The first message transmission means determine the authenticator and the checking means determine the check value based on the selected key.

Claim 14, upon which claims 15-16 are dependent, recites an authentication method for a telecommunications network. The method includes generating a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key. The method also includes transmitting at least some of the challenges contained in the authentication data blocks to a terminal. The method also includes receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal. The method also includes determining based on said data unit which challenge was chosen by the terminal. The

method also includes determining a check value with a key corresponding to the chosen challenge. The check value is compared with the authenticator.

Claim 17, upon which claims 18 and 19 are dependent, recites an authentication method for a terminal. The method includes receiving a set of challenges from a telecommunications network. The method also includes choosing one challenge from the set of challenges. The method also includes determining a response and a key based on the chosen challenge. The method also includes determining an authenticator based on the key corresponding to the chosen challenge. The method also includes transmitting the authenticator and the data unit to the telecommunications network. The data unit relates to the manner in which the authenticator is formed. The method also includes notifying the telecommunications network of the chosen challenge.

Claim 20 recites a telecommunications network configured to generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key. The network also is configured to transmit at least some of the challenges contained in the authentication data blocks to a terminal. The telecommunications network also is configured to receive an authenticator and a data unit containing information relating to a manner in which the authenticator is formed. The telecommunications network also is configured to determine based on the data unit which challenge was chosen by the terminal. The telecommunications network also is configured to determine a check value with the key correspondent to the chosen challenge. The check value is compared with the authenticator.

Claim 21 recites terminal for a telecommunications network. The terminal is configured to receive a set of challenges from a telecommunications network. The terminal is also configured to choose one challenge from a set of challenges. The terminal also is configured to determine a response and a key based on the chosen challenge. The terminal also is configured to determine an authenticator based on the key corresponding to the chosen challenge. The terminal also is configured to transmit the authenticator and the data unit to the telecommunications network. The data unit relating to the manner in which the authenticator is formed and notifies the telecommunications network of the chosen challenge.

As discussed in the specification, examples of the present invention enable the use of a known authentication method of a telecommunications network for producing an authenticator for a terminal. Examples of the present invention enable a terminal to receive a challenge and to determine a corresponding key and response. The response is sent from the terminal to the network, where the response received from the terminal is compared to the response calculated in the network. If these two responses are equal, the terminal is successfully authenticated. Thus, it is possible to share a secret key between the terminal and the network for calculating an authenticator in the terminal and for checking the authenticator network. The authenticator may be calculated using any method, which has been, for example, agreed upon before hand. The network is notified about the chosen challenge using a data unit. Applicant respectfully submits that Li and Scott, either alone or in combination, fail to disclose or suggest all the features of any of

the presently pending claims. Therefore, Li and Scott fail to provide the critical and unobvious advantages discussed above.

Li relates to a method of using fingerprints to authenticate wireless communications. Figure 5 of Li shows software processing steps for fingerprint matching. A contrasting algorithm reduces all the gray shades of a captured image 502 to either black for ridgelines or white for valley lines, as shown in image 504. A thinned image 506 is examined by further algorithms in step 507 that attempt to deduce and accurately extract the minutiae and their locations as shown in a map 508. Figure 6 of Li shows a diagram of central authentication system (CAS) 106. CAS 106 includes a memory 605 including a persistently stored program 606 and various temporarily stored items including a challenge 607, a response token 608, and a decrypted message 609. Program 606 contains instructions for generating a challenge, encrypting the challenge with a fingerprint based token, validating a decrypted challenge by comparison with the generated challenge, fingerprint matching based on tokens, and comparing a response token with one or more stored tokens to assure that tokens are not identical to imply illegal use.

Scott relates to continuous authentication using an in-band or out-of-band side channel. Scott describes a re-authentication procedure between the modems of a public switched telephone network (PSTN) data connection between a computer facility and a user. Referring to Figure 3 of Scott, CPU 210 receives the originating modem's ID number. CPU 210 proceeds to step 320 and retrieves, from key list 221, a corresponding

data encryption key. Key list 221 is stored in memory 220 a priori, and represents a plurality of modem ID numbers, each of which represents a possible originating modem. Each modem ID number is associated with a data encryption key. The associated data encryption key, like the modem ID, also is determined a priori in the originating modem. CPU 210 randomly generates a number, which is known as a challenge in step 325. Upon receiving the challenge from modem 200, modem 120 encrypts the challenge, via its data encryption processor to generate a response, or a form of "cipher text" that is sent back to modem 200. The encryption performed by modem 120 uses its stored data encryption key. Figure 4 of Scott also shows the authentication process where answering modem 200, the grantor, transmits a "send modem ID" message 605 to originating modem 120, the requestor, which responds by transmitting "ID" 610. Answering modem 200 transmits "challenge" 615 to originating modem 120, which transmits "response" 620.

Applicant submits that Li and Scott, either alone or in combination, fail to disclose or suggest all the features of any of the presently pending claims. For example, Li and Scott fail to disclose or suggest generating a set of subscriber-specific authentication data blocks in the network, each data block containing a challenge, a response and a key. Li describes a challenge and a response where the response is a challenge modified based on fingerprint information. Li fails to disclose or suggest generating a set of subscriber-specific authentication data blocks that include a challenge, a response and a key.

Further, Li fails to disclose or suggest transmitting at least some of the challenges contained in the authentication data blocks to the terminal. Li describes a challenge encrypted with fingerprint information that is sent to the source, such as a wireless telephone. Li fails to send challenges to the terminal. Li also fails to disclose or suggest choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used. Instead, Li describes receiving the encrypted challenges one at a time at the source. Applicant notes that the encrypted challenges of Li are not received at the terminal, and, as such, the challenges also are not chosen at the terminal.

Li also fails to disclose or suggest determining an authenticator with an aid of the chosen key in the terminal. Li describes receiving a decrypted challenge from the source. The challenge of Li that was encrypted with fingerprint information available to the network is decrypted in the source using fingerprint information available to the source. The decrypted challenge of Li from the source is an authenticator. Thus, applicant submits that the authenticator of Li is based on information, such as fingerprint information, and not on a key relating to a chosen challenge. Thus, the authenticator of Li is not derived from a key. Thus, Li fails to determine an authenticator with an aid of a chosen key in the terminal.

Li also fails to disclose or suggest determining a check value with the aid of the chosen key in the network. Li describes sending one encrypted challenge at a time from the network to the source, such as a wireless telephone, and then the source sends a

decrypted challenge to the network for comparing the original challenge to the received decrypted challenge. Li does not determine a check value. Further, the comparing described in Li does not result in a chosen key. Applicant maintains that Li fails to disclose or suggest at least these features of the claims.

Applicant submits that Scott, either alone or in combination with Li, fails to disclose or suggest the features of the claims missing from Li. The Office Action alleges that Scott teaches "generating a set of subscriber specific authentication data blocks into the network, each data block containing a challenge, a response and a key." Applicant asserts that Scott describes using a plurality of challenges and a plurality of responses where one random number, or challenge, is sent at a time to the calling modem. Scott fails to disclose or suggest sending some challenges to a terminal and then having the terminal choose one of the challenges for use in the terminal. Further, applicant submits that the random number challenges of Scott are distinguishable from the data blocks, as claimed. For example, the random number challenges of Scott fail to include a challenge, a response and a key. Applicant maintains that Scott, like Li, does not disclose or suggest a key that is used to determine an authenticator.

In contrast, claim 1 of the present invention recites "generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communications system" and "choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be

used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communications system, determining an authenticator with an aid of the chosen key in the terminal." Claim 10 is directed to an authentication system, and recites some common features with claim 1. Claim 14 recites "transmitting at least some of the challenges contained in the authentication data blocks to a terminal, determining based on said data unit which challenges chosen by the terminal, and determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator."

Claim 17 recites "receiving a set of challenges from a telecommunications network, choosing one challenge from the set of challenges, determining the response in the key based on the chosen challenge, and determining an authenticator based on the key corresponding to the chosen challenge." Claim 20 is directed to a telecommunications network, and recites some features in common with claim 14. Claim 21 is directed to a terminal for a telecommunications network, and recites some of the features of claim 17. Applicant respectfully submits, for the reasons given above, that Li and Scott fail to disclose or suggest at least these features of the presently pending claims.

Because the cited references, either alone or in combination, do not disclose or suggest all the features claims 1, 10, 14, 17, 20 and 21, then claims 1-21 are not rendered obvious. The dependent claims also are not disclosed or suggested by the cited references at least because of their dependency upon the independent claims, and the fact that they recite additional subject matter not disclosed or suggested by the cited

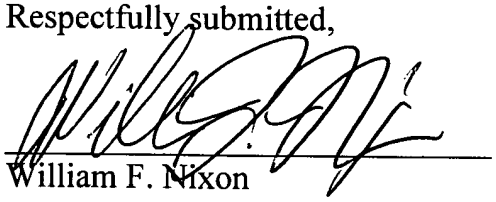
references. Applicant respectfully requests that the obviousness rejection for claims 1-21 be withdrawn.

Applicant submits that each of claims 1-21 recite subject matter that is neither disclosed nor suggested by the cited references, either alone or in combination. Applicant respectfully requests that all of claims 1-21 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



William F. Nixon
Registration No. 44,262

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802
WFN:cct